

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE UNITED STATES ARMY CYBER CENTER OF EXCELLENCE (CYBER COE)
AND
BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA ON
BEHALF OF AUGUSTA UNIVERSITY
FOR
COLLABORATION IN PROVIDING EDUCATION, TRAINING, RESEARCH, AND
OUTREACH

Cyber CoE #16-266

This is a Memorandum of Understanding (MOU) between the United States Army Cyber Center of Excellence (Cyber CoE) and Augusta University. When referred to collectively, they are referenced to as the "Parties."

1. BACKGROUND:

1.1. The goal of this MOU is to establish an academic-government partnership that enables the growth of a cyber-capable workforce that meets local, regional, national, and society cyber workforce needs as well as assist local cyber economic development, innovation and research, and take advantage of Augusta University's already well developed medical data privacy and big data analytics experience.

1.2. REFERENCES:

1.2.1. Department of Defense Instruction (DoDI) 4000.19, Support Agreements, 25 APR 2013.

1.2.2. Department of Defense University Affiliated Research Center (UARC) Management Plan, 23 JUN 2010.

1.2.3. Department of Defense Strategy for Operating in Cyberspace, JUL 2011.

1.2.4. Georgia Regents University Strategic Plan – Transition Forward 2013.

1.2.5. Department of Defense Cyberspace Workforce Strategy, 04 DEC 2013.

1.2.6. The Department of Defense Cyber Strategy, APR 2015.

1.2.7. Establishment of the Georgia Regents University Cyber Institute – May 2015.

1.2.8. University System of Georgia Cybersecurity Initiative -- Insights from

the Field, 12 AUG 2015.

1.2.9. United States Army Cyber Center of Excellence Strategic Plan, SEP. 2015.

1.2.10. Georgia Regents University Cyber Institute Initiatives/Fact Sheet – October 2015.

2. AUTHORITIES: 10 u.s.c.2304(c)(3)(B)

3. PURPOSE: U.S. Army Cyber Center of Excellence (CoE) is pursuing a long-term, strategic partnership with Augusta University to access educational, training, technical, research and outreach resources in support of Cyber CoE's mission.

This MOU between Augusta University and the U.S. Cyber CoE is for the purpose of fostering a strategic relationship between said parties. The MOU also describes the objectives and scope of Augusta University provided collaboration and future education, training, technical, research and outreach support for Fort Gordon's mission to be the Department of Defense's recognized experts for cyberspace operations. This MOU establishes the basic assumptions required to enable effective collaboration and support requirements. Each of the undersigned parties understand and agree to support the objectives and uphold the responsibilities outlined in this MOU.

Hereinafter, the term "Institution" will refer to the collective Augusta University applicable entities within the degree and non-degree granting organizations.

The objective of this MOU is to establish a mutually beneficial, cooperative relationship between Augusta University and U.S. Cyber CoE for purposes including but not limited to:

3.1. Developing a nationally recognized cyber education, training and support capability.

3.2. Developing educational programing, training, and technical support in mutual areas of interest to the Parties. Examples of possible programs include region of interest pre-deployment briefings, Cyberspace Defense and Cyberspace Operations certificate programs, undergraduate programs in computer science and information technology, graduate programs in cyber security, computer science, health informatics analytics and intrusion detection, Public Administration with a Homeland Security track, and International Studies (includes a specific Middle Eastern Security Studies course), use of electromagnetic spectrum or directed energy to control the spectrum.

3.3. Collaborating on and/or co-developing applicable cyberspace capabilities to

support Training and Doctrine Command (TRADOC) Capabilities Manager-Cyber (TCM-Cyber) and the Cyber/Network Battle Lab, as the user representative and experimentation support, respectively, for U.S. Army Cyberspace Command (ARCYBER) Joint Force Headquarters -Cyber (JFHQ-C), and other Army cyberspace stakeholders (to include corps and below elements).

3.4. Jointly pursuing appropriate training, mission support, and participation in early acquisition insight test/experimentation venues.

3.5. Exploring internships and participation of students/trainees in relevant activities at each site represented by the Parties.

3.6. Developing and executing formalized agreements and contractual documents between the parties, such as Education Partnership Agreement, Cooperative Research and Development Agreement (CRADA), cooperative agreement, UARC contract, DOD Information Analysis Center (IAC) Technical Area Task (TAT), or similar contractual vehicle to facilitate Institution support to Fort Gordon stakeholders.

4. Responsibilities of the Parties:

4.1. The Cyber CoE will –

4.1.1. Assist in Institution curriculum development and participate as instructors during seminars and short courses when appropriate.

4.1.2 Provide facilities and equipment in support of these educational programs as needed and agreed upon.

4.1.3. Ensure students meet designated security classification requirements for the course.

4.1.4. Facilitate internships for degree, non-degree and professional education trainees and students.

4.1.5. Collaborate with the Institution in order to determine future initiatives and research areas of mutual interest, including cyber outreach initiatives.

4.1.6. Provide an opportunity/avenue for the Institution to advertise and educate the Fort Gordon cadre regarding available Institute educational opportunities on a quarterly basis.

4.1.7. Support Augusta University efforts to advertise cyber adjunct faculty opportunities.

4.2. The Institution will–

4.2.1. Develop professional education short courses of mutual benefit and facilitate undergraduate/graduate educational opportunities with the degree-granting organizations within the Institution to meet the needs of the U.S. Army Cyber CoE.

4.2.2. Educational offerings include but are not limited to:

4.2.2.1. Short Courses: Cyber Defender Certificates and Continuing Education Units from Augusta University

Examples of courses currently offered as part of Augusta University's Cyber Defender Certificate program are:

Principles of Computer Programming

Principles of Computer Programming II

Introduction to Computer Networking

System Administration

Introduction to Cyber Security

Database Management Systems

Introduction to Defensive Cyber Operations

Cyber Network Defense and Counter Measures

Digital Forensics

Operating Systems

Assembly Programming

TCP/IP Protocol Analysis

Reverse Engineering

Undergraduate Research

Ethics in Computer Science

White Collar Crime

Project Management

Management Information Systems

Visual Communications

4.2.2.2. Degree Programs:

BS in Computer Science

BS in Applied Information Systems and Technologies (IT)

Masters in Public Administration with a Homeland Security track

Masters of Public Health with a concentration in Health Informatics

4.2.3. Enable Army professional educator collaboration with the Institute's Faculty Development and Teaching Excellence Center as well as the College of Education as desired by the U.S. Cyber CoE.

4.2.4. Brief and initiate the evaluation/enrollment process for new students prior and during all new Cyber training start-up sessions.

4.2.5. During Cyber Student Graduation ceremonies, the Institution shall be on hand to present an official institutional certificate of training and possible transcripts containing the regional awarded college credit (if applicable) for the dual enrolled courses and/or residential on-line institutional required courses.

4.3. To meet the objectives described above, BOTH PARTIES agree to:

4.3.1. Identify a senior Institution faculty member and Cyber CoE senior leader as the principal points of contact (or liaisons) in each party to apprise the MOU signatories with the progress of collaboration.

4.3.2. Work towards creating accredited articulated cooperative (program) both covering Cyber degrees and certificates of training.

4.3.3. Identify ways for non-degree seeking students to enroll in credit courses.

4.3.4. Co-sponsor an annual cyber security training event (e.g., workshop, exercise, conference, etc.) at the Institution or at Fort Gordon.

4.3.5. Establish quarterly meetings (alternating between locations or by conference/ teleconference VTC/online participation if agreeable to both parties). The intent is to provide representatives from all organizations the opportunity for ongoing information sharing regarding current, planned, and/or new initiatives and activities.

4.3.6. Meet annually to review activities of the past year, and plans for the following year.

4.3.7. Explore the implementation of an on-line co-enrollment with the Institution when Service members are assigned to Fort Gordon for formal Cyber and/or Signals training.

4.3.8. When needed, develop and execute between the parties a contractual vehicle(s) to facilitate timely Augusta University support to Fort Gordon stakeholders.

4.3.9. Adhere to each party's respective security rules and regulations when courses, meetings and conferences are hosted at Cyber CoE and the Institution.

5. PERSONNEL: Each Party is responsible for all of its personnel costs including pay and benefits, support, and travel. Each Party is responsible for supervision and management of its personnel; there will be no shared responsibility for management and/or supervision of personnel.

6. GENERAL PROVISIONS:

6.1. POINTS OF CONTACT: The Parties will use the following Points of Contact (POC) in the implementation of this MOU. Each Party may change its POC upon reasonable notice to the other Party.

6.1.1. For the Cyber CoE-

Primary POC: Ms. Gloria Palmer, G-8, (706) 791-8753,
gloria.m.palmer2.civ@mail.mil.

Alternate POC: Ms. Kimberly Burr, DOT, (706) 791-5482,
kimberly.m.burr.civ@mail.mil

6.1.2. For the Institution-

Primary POC: Ms. Joanne Sexton, Director of Cyber Institute,
(706) 729-2351, js Sexton1@gru.edu

Alternate POC: Ms. Karyn Nixon, Government & Community Affairs,
(706) 721-2335, knixon@gru.edu

6.2. CORRESPONDENCE: The Parties will address all written correspondence sent or received specific to the content of this MOU as follows, unless directed otherwise:

6.2.1 For the Cyber CoE-

Primary POC: Ms. Gloria Palmer, G-8, (706) 791-8753

gloria.m.palmer2.civ@mail.mil
Alternate POC: Ms. Kimberly Burr, DOT, (706) 791.5482
kimberly.m.burr@mail.mil

6.1.2. For the Institution-

Primary POC: Ms. Joanne Sexton, Director of Cyber Institute,
(706) 729-2351, jsexton@gru.edu
Alternate POC: Ms. Karyn Nixon, Government & Community Affairs,
(706) 721-2335, knixon@gru.edu

6.3. MODIFICATION OF UNDERSTANDING: This MOU may only be modified by the written agreement of the Parties, duly signed by their authorized representatives. Such amendments will be dated, consecutively numbered, and appended to each copy of this document.

6.4. DISPUTES: Any disputes relating to this MOU will, subject to any applicable law, Executive Order, Directive, or Instruction, be resolved by consultation between the Parties or in accordance with DoD 4000.19.

6.5. TERMINATION OF UNDERSTANDING: Either party may unilaterally terminate the agreement prior to the expiration date only with sufficient advance notification, a minimum of 180 days, to permit appropriate resource adjustments to be made during the budget formulation process. If an agreement involves reimbursement or if resources must be significantly modified or unilaterally terminated with less than 180 days' notice to the other party or parties to the agreement, the party requiring the modification or termination may be billed by the supplier in accordance with the terms of the applicable agreement for reimbursement. If there are no agreements in place and there are no outstanding issues involving reimbursement, this MOU may be unilaterally terminated by either party prior to the expiration date by providing 30 days of advance notification. The MOU may also be terminated at any time upon the mutual written consent of the Parties.

6.6. TRANSFERABILITY: This MOU is not transferable except with the written consent of the Parties.

6.7. ENTIRE UNDERSTANDING: It is expressly understood and agreed this MOU embodies the entire agreement between the Parties regarding the MOU's subject matter.

6.8. EFFECTIVE DATE: This MOU takes effect beginning on the day after the signature of the last Party.

6.9. EXPIRATION DATE: This MOU expires nine years and one day after

the signature of the last Party. If the agreement is to remain in effect after the nine-year period, it can be re-signed in conjunction with the third triennial review.

6.10. CANCELLATION OF PREVIOUS AGREEMENT: N/A

7. FINANCIAL DETAILS:

7.1. AVAILABILITY OF FUNDS: This MOU does not document the obligation of funds between the Parties. Any obligation of funds in support of this MOU will be accomplished as mutually agreed to by both Parties. The obligation of the funds by the Parties is subject to the availability of appropriated funds pursuant to the DoD Financial Management Regulation.


7.2. BILLING: The Institution will bill the lead organizations, as designated by the Cyber COE, in accordance with the procedures established for products and/or services in the applicable Program Level Agreements (PLA) or as otherwise agreed upon by supplemental negotiation between the Parties. The Parties will maintain a record of the transactions by written/electronic correspondence between the Parties or by annual report after the month in which the first transaction occurred. Billing will be established in the applicable PLA or as otherwise agreed to by the Parties.


7.3. PAYMENT OF BILLS: Reimbursement will occur as mutually negotiated within the structure of the individual PLAs.

7.4. FINANCIAL SPECIFICS: See the applicable PLA(s) established in regard to agreed upon products and services or other supplemental agreements for details and information on the reimbursable support identified pursuant to the responsibilities identified in paragraph 4 of this MOU.

AGREED:

BOARD OF REGENTS OF THE
UNIVERSITY SYSTEM OF GEORGIA
ON BEHALF OF AUGUSTA UNIVERSITY


BROOKS A. KEEL, Ph.D.
President, Augusta University,


STEPHEN G. FOGARTY
Major General, U.S. Army
U. S. Army CYBER Center of
Excellence

